GCED Q&As

GIAC Certified Enterprise Defender Practice Test

Pass GIAC GCED Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/gced.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

In an 802.1x deployment, which of the following would typically be considered a Supplicant?

A. A network switch

B. A perimeter firewall

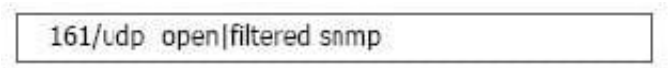
C. A RADIUS server

D. A client laptop

Correct Answer: D

QUESTION 2

When running a Nmap UDP scan, what would the following output indicate?



A. The port may be open on the system or blocked by a firewall

B. The router in front of the host accepted the request and sent a reply

C. An ICMP unreachable message was received indicating an open port

D. An ACK was received in response to the initial probe packet

Correct Answer: A

Explanation: When Nmap shows an "open filtered" response for the scan results, this indicates a couple of different reasons. The port could be open but a firewall could be blocking the use ACK flags; only TCP

packets do.

QUESTION 3

You are responding to an incident involving a Windows server on your company\\'s network. During the investigation you notice that the system downloaded and installed two files, iexplorer.exe and iexplorer.sys. Based on the behavior of the system you suspect that these files are part of a rootkit. If this is the case what is the likely purpose of the .sys file?

A. It is a configuration file used to open a backdoor

B. It is a logfile used to collect usernames and passwords

C. It is a device driver used to load the rootkit

D. It is an executable used to configure a keylogger

Correct Answer: C

QUESTION 4

What is needed to be able to use taskkill to end a process on remote system?

A. Svchost.exe running on the remote system

B. Domain login credentials

C. Port 445 open

D. Windows 7 or higher on both systems

Correct Answer: B

Explanation: Domain login credentials are needed to kill a process on a remote system using taskkill.

QUESTION 5

Requiring criminal and financial background checks for new employees is an example of what type of security control?

A. Detective Support Control

B. Detective Operational Control

C. Detective Technical Control

D. Detective Management Control

Correct Answer: D

Explanation: Management Controls include: Policies, guidelines, checklists, and reporting.

Detective management controls include personnel security. As a detective control, we are referring to

indepth background investigations, clearances, and rotation of duties.